Section V:	**Physical Security**
Title:	**Facility Perimeter Security Standard**
Current Effective Date:	**June 30, 2008**
Revision History:	**May 16, 2008**
Original Effective Date:	**June 30, 2008**

Purpose: To define perimeter security and provide guidance for Divisions and Offices of the North Carolina (NC) Department of Health and Human Services (DHHS) on implementing protection measures to deter, detect, and respond to unauthorized facility access.

STANDARD

1.0 Background

Perimeter security controls are a necessary step to accomplishing a secure environment to maintain information security systems and protect data that is created or maintained by an organization. The strength of the perimeter security controls an organization needs to employ should be based on a current risk assessment.

2.0 Defining the Facility Perimeter

The facility perimeter is considered to be the area starting at the building exterior and extending outward to the area over which the organization can implement physical safeguards. Structures may be erected or controls used within the outermost perimeter boundary to create multiple perimeter zones.

3.0 Perimeter Control Considerations

There are several circumstances that must be considered when evaluating the need for and use of perimeter controls. The following is a partial list of considerations:

- Perimeter controls should be governed by a risk assessment of the facility, the assets within and the externally exposed information technology (IT) asset support services (i.e., communication lines, power lines, etc.)
- Modification to the facility and surrounding environment will be subject to the property rights that an entity has over the property
- Facility purpose or location may present aesthetic concerns (i.e., limited changes that can be made to historical buildings)
- Local ordinances may limit the use of certain controls
- All perimeter controls must comply with appropriate federal, state, and local human safety and accessibility regulations and requirements
- Personnel and equipment access must not be hindered during response to an emergency because of perimeter security measures implemented

4.0 Perimeter Threats and Controls

Threats such as building intrusions, vandalism, theft, etc., should be analyzed as a part of a comprehensive security plan. The following is a partial list of vulnerabilities that allow building entry or service interruption and should be included in a risk assessment and considered when constructing a perimeter security plan:

- Exposed/unsecured door hinges
- Breakable glass entry doors
- Lack of entry point monitoring or intrusion detection system
- Unlit areas or obstacles that enable unsuspected attacks
- Unobstructed vehicular access to the building
- Unprotected windows less than 18 feet above the ground
- Unprotected conduit entry points greater that 96 square inches
- Unprotected telecommunications/data trunks, HVAC systems and utilities

The following is a partial list of controls available to mitigate threats and vulnerabilities:

- Restricted area warning signs, walls, bollards, fences, closed circuit television (CCTV), or guard patrols
- Perimeter conduit grates, window bars or baffles, man hole cover locks
- Exterior lighting and removal or relocation of objects that enable unsuspected attacks
- Multiple perimeter zones, electronic entry control systems, and manned reception areas
- Exterior doors with no glass panels or break resistant glass
- Perimeter intrusion detection systems

5.0 Responsibility for Perimeter Control

Divisions and Offices must designate an individual to be responsible for working with the NC DHHS Property and Construction or applicable agency to plan and implement appropriate perimeter controls. That person shall identify and recommend controls that reduce risks to acceptable levels. Acceptable levels will vary depending on the type of threats anticipated for the facility based on a risk assessment. The assigned individual is responsible for ensuring all aspects of perimeter controls are managed according to policy, procedures, and standards.

6.0 Maintenance and Testing of Perimeter Controls

Periodic servicing and operational testing of perimeter controls is essential to providing assurance of both functional performance and integrity of the safeguards. A physical security inspection shall be performed periodically by a designated Division or Office workforce member to evaluate the adequacy of the risk assessment as well as the appropriateness and effectiveness of the perimeter controls implemented. The inspection shall be coordinated with the DHHS Office of Property and Construction or applicable agency, and the DHHS Safety Director.

A maintenance and inspection schedule must be developed for each perimeter control system. A record of inspection and maintenance must be retained. When a perimeter control system is installed, replaced, or repaired, maintenance records will be updated to reflect the date of installation.

7.0 Maintenance Schedule and Repair Records

For information on retaining maintenance schedules, repair, and systems records, refer to the NC DHHS Policy and Procedures Manual, Section VIII - Security and Privacy, Security Manual, Physical and Environmental Security Policy.

8.0 Perimeter Control System Safety Precautions

Divisions and Offices shall develop procedures to allow for controlled facility access while at the same time allowing safe exit from the facility during emergencies or system failures. For example, all facility entry/exit doors must be equipped with crash bar latches to allow for unimpeded egress during an evacuation.

Reference:

- HIPAA Administration Simplification - Act 45 C.F.R. Part 160 and 164.
  - HIPAA - 45 C.F.R. § 164.310(a)(2) Implementation specifications.

- NC Statewide Information Security Standards Version No. 1
  - Chapter 3 - Processing Information and Documents, Section 02: System Operation and Administration
    - Standard 030215 - Commissioning Facilities Management for Information Technology
  - Chapter 9 - Dealing with Premises Related Considerations, Section 01: Premises Security –
    - Standard 090102 - Securing Physical Protection of Computer Premises
  - Chapter 9 - Dealing with Premises Related Considerations, Section 03: Other Premises Issues
    - Standard 090303 - Disaster Recovery Plan

- NC DHHS Policy and Procedures Manual, Section VIII - Security and Privacy, Security Manual,
  - Physical and Environmental Security Policy
  - Security Testing Policy